(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
1 août 2002 (01.08.2002)

PCT

(10) Numéro de publication internationale
WO 02/059845 A1

(51) Classification internationale des brevets[7] : G07F 7/10

(21) Numéro de la demande internationale :
PCT/FR02/00306

(22) Date de dépôt international :
25 janvier 2002 (25.01.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/01100 26 janvier 2001 (26.01.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F-13881 Gémenos (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **TOURNIER, Didier** [FR/FR]; 12, rue du Loisir, F-13001 Marseille (FR).

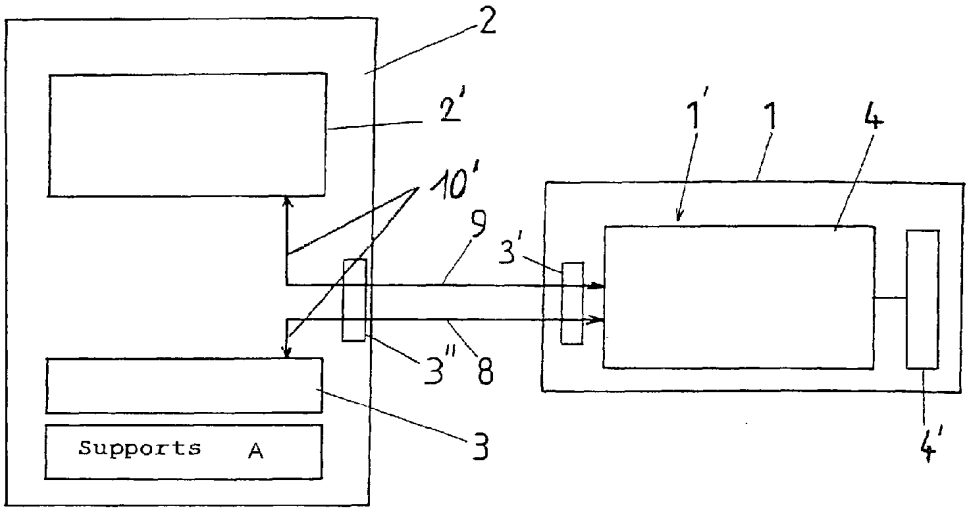
(74) Mandataire : **MILHARO, Emilien**; c/o GEMPLUS, Av du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: INTEGRATED CIRCUIT CARD OR SMART CARD INCORPORATING A SECURITY SOFTWARE CARD AND COMMUNICATION DEVICE CO-OPERATING WITH SAME

(54) Titre : CARTE A CIRCUIT(S) INTEGRE(S) OU CARTE A PUCE(S) INTEGRANT UNE COUCHE LOGICIELLE DE SECURISATION ET DISPOSITIF DE COMMUNICATION COOPERANT AVEC UNE TELLE CARTE



A...MEDIA

(57) Abstract: The invention concerns an integrated circuit card (1) comprising a connection and communication interface (3') designed to set up a communication with a host unit (2) in the form of a communication device and cryptographic software means (4') for cryptographic calculations. Said card (1) is characterised in that the integrated circuit(s) (1') further comprise(s) a security or security-providing software layer (4) designed to co-operate with said cryptographic software means (4') to produce a set of security operations on the received data and to transmit via the connection and communication interface (3') of said card (1).

[Suite sur la page suivante]

WO 02/059845 A1

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : La présente invention concerne une carte (1) à circuit(s) intégré(s) comportant une interface (3') de connexion et de communication destinée à établir une communication avec une unité hôte (2) sous la forme d'un dispositif de commnication et des moyens logiciels cryptographiques (4') pour réaliser des calculs cryptographiques. Carte (1) caractérisée en ce que le(s) circuit(s) intégré(s) (1') comporte(nt) en outre une couche logicielle de sécurité ou sécuritaire (4) apte à coopérer avec lesdits moyens logiciels cryptographiques (4') pour réaliser un ensemble d'opérations sécuritaires sur les données reçues et à émettre via l'interface de connexion et de communication (3') de ladite carte (1).

CARTE A CIRCUIT(S) INTEGRE(S) OU CARTE A PUCE(S) INTEGRANT UNE COUCHE LOGICIELLE DE SECURISATION ET DISPOSITIF DE COMMUNICATION COOPERANT AVEC UNE TELLE CARTE

La présente invention concerne le domaine des transmissions par des moyens de communications de données sécurisées.

L'invention concerne notamment les services fournis par les communications basées sur le protocole internet ("WWW"), et a pour objet une carte à circuit(s) intégré(s) permettant de sécuriser de telles transmissions, un dispositif de communication apte à coopérer avec une telle carte, un dispositif formé par l'association du dispositif et de la carte précités et un système de communication comprenant au moins un tel dispositif.

Dans la présente demande, le terme carte à circuit(s) intégré(s) ou à puce(s) s'applique à tout support notamment plan en forme de plaque et en matière thermoplastique, renfermant au moins un circuit intégré du type microprocesseur associé à une mémoire et à des bornes de contact en surface. Ces cartes présentent une taille adaptée à la fente de réception de l'unité hôte ou du module de connexion associé à cette dernière et destiné à recevoir temporairement ladite carte. Ces cartes sont généralement attribuées chacune de manière personnelle et unique à un possesseur et utilisateur individuel et assorties chacune d'un code confidentiel connu de l'utilisateur seul.

Des exemples types, mais non limitatifs, de telles cartes sont les cartes de paiement ou cartes bancaires.

Il est déjà connu d'utiliser les cartes à puce(s) ou cartes dites "intelligentes" comme composant accessoire amovible pour authentifier ou sécuriser les données émises ou reçues par une unité hôte, tel qu'un ordinateur, un téléphone cellulaire, un assistant personnel électronique, ou une unité de traitement de données et de communication ou analogue.

Ces cartes remplissent soit uniquement un rôle purement esclave de fournisseur d'une clé de session, soit en plus un rôle actif en tant qu'unité esclave sous le contrôle des moyens logiciels implantés dans l'unité hôte et mis en œuvre par cette dernière pour fournir à l'utilisateur les services requis par lui. Dans ce dernier cas, la carte réalise un certain nombre de procédures de calculs cryptographiques (vérification de certificats, calcul d'une clé de session, génération de signature, hachage, codage, décodage...) à la demande et en fonction des nécessités, par

exemple, d'un navigateur, d'un explorateur, d'un logiciel de courrier électronique ou d'une entité logicielle d'une couche de communication ou de sécurité. Les logiciels résidents précités de l'unité hôte font exécuter à la carte des calculs cryptographiques dont ils ont besoin pour la couche sécuritaire implantée dans l'unité hôte, afin que cette dernière puisse réaliser l'ensemble des opérations sécuritaires requises.

Un exemple d'architecture générale d'une telle association unité hôte /carte est représenté schématiquement sur la figure 1 (logiciels résidents 2').

Dans la présente demande, on entend par le terme "ensemble des opérations sécuritaires", l'ensemble des opérations nécessaires pour échanger des données sécurisées avec une unité distante dite sécurisée. Il s'agit, en particulier, de l'ensemble des fonctions algorithmes que l'on retrouve actuellement dans la couche sécuritaire d'un protocole de communication de type internet.

Cette couche de sécurité ou sécuritaire peut être, par exemple, du type SSL (Secure Sockets Layer - couche de connexion sécuritaire), TLS (Transport Layer Security - couche de transport sécuritaire) ou encore WTLS (Wireless Transport Layer Security - couche de transport radio sécuritaire).

Les protocoles de transmission mis en œuvre au niveau de l'interface de communication 3 pourront, par exemple, être du type connu sous la désignation UDP (pour User Datagram Protocol) ou sous la désignation TCP (toutes deux liées aux couches IP).

Toutefois, un risque majeur résulte de ces utilisations du fait de l'export de la clé de session vers l'unité hôte (par exemple pour l'encryptage), à savoir que ladite clé de session peut être piratée par des logiciels du type connu sous la désignation "Cheval de Troie" et que des informations erronées peuvent être générées.

En outre, du fait de l'implantation de la couche de sécurité dans l'unité hôte, son éventuelle évolution, pour tenir compte de la nécessaire évolution des techniques sécuritaires, est directement liée à une modification plus générale des logiciels installés ou même à un changement de l'unité hôte, notamment en ce qui concerne les produits grand public.

Il peut résulter un retard important entre les techniques de piratage à l'évolution rapide et la couche sécuritaire obsolète installée dans

l'unité hôte, rendant cette dernière extrêmement vulnérable en cas de communication avec l'extérieur.

Enfin, une personnalisation et une adaptation des mesures sécuritaires en fonction de l'utilisateur n'est généralement pas disponible au niveau de l'unité hôte.

La présente invention vise notamment à surmonter au moins certaines des limitations et à pallier certains des inconvénients précités.

A cet effet, la présente invention a pour principal objet une carte à circuit(s) intégré(s) comportant une interface de connexion et de communication destinée à établir une communication avec une unité hôte sous la forme d'un dispositif de communication et des moyens logiciels cryptographiques pour réaliser des calculs cryptographiques, carte caractérisée en ce que le(s) circuit(s) intégré(s) comporte(nt) en outre une couche logicielle de sécurité ou sécuritaire apte à coopérer avec lesdits moyens logiciels cryptographiques pour réaliser un ensemble d'opérations sécuritaires sur les données reçues et à émettre via l'interface de connexion et de communication de ladite carte.

L'invention sera mieux comprise, grâce à la description ci-après, qui se rapporte à un mode de réalisation préféré, donné à titre d'exemple non limitatif, et expliqué avec référence aux dessins schématiques annexés, dans lesquels :

la figure 2 est une représentation schématique (schéma blocs) d'une architecture possible d'une unité hôte et de la carte pouvant être associée à cette dernière selon une première variante de réalisation de l'invention ;

la figure 3 est une représentation schématique similaire à celle de la figure 2 intégrant une seconde variante de réalisation de la carte selon l'invention ;

la figure 4 est une variante de réalisation de l'architecture d'une unité hôte faisant partie d'un dispositif similaire à ceux représentés sur les figures 1 et 2, et,

la figure 5 est un ordinogramme montrant un exemple de procédure de mise en communication basée sur le protocole WAP (Protocole d'application radio).

La présente invention concerne en premier lieu une carte 1 à circuit(s) intégré(s) 1' comportant une interface 3' de connexion et de communication destinée à établir une communication avec une unité hôte 2

sous la forme d'un dispositif de communication et des moyens logiciels cryptographiques 4' pour réaliser des calculs cryptographiques.

Cette carte est caractérisée en ce que le(s) circuit(s) intégré(s) 1' comporte(nt) en outre une couche logicielle de sécurité ou sécuritaire 4 apte à coopérer avec lesdits moyens logiciels cryptographiques 4' pour réaliser un ensemble d'opérations sécuritaires sur les données reçues et à émettre via l'interface de connexion et de communication 3' de ladite carte 1.

Ainsi, la carte selon l'invention a l'avantage d'éviter l'export de la clé de session à l'extérieur, puisque ladite carte comporte elle-même la couche logicielle de sécurité que l'on trouvait généralement dans l'unité hôte. De ce fait les communications sont plus sécurisées.

La carte 1 comporte avantageusement une mémoire pour le stockage de la clé de session (ou clé de chiffrement/déchiffrement) dont l'accès en lecture est uniquement autorisé pour ladite couche de sécurité 4 de la carte 1 de manière à éviter l'accès par des moyens externes à la carte.

Selon une première caractéristique de l'invention, la couche logicielle de sécurité 4 comporte une fonction ou un groupe de fonctions permettant une négociation d'algorithme et de clé, ainsi qu'une fonction de chiffrement et déchiffrement et, le cas échéant, en outre une fonction d'authentification de certificat.

De manière avantageuse, ladite couche logicielle de sécurité 4 est, en coopération avec lesdits moyens logiciels cryptographiques 4', apte à réaliser un ensemble d'opérations sécuritaires permettant une sécurité de communication de type "internet".

De plus, cette couche 4 est préférentiellement choisie dans le groupe formé par les couches de type SSL, TLS, WTLS ou analogue.

En cas de sollicitation, ladite couche logicielle de sécurité 4 est apte à traiter la totalité, ou le cas échéant au moins une partie, des flux de données entrant et sortant par au moins une interface de communication 3 de ladite unité hôte 2 assurant la connexion de cette dernière à un réseau de communication, en réalisant les opérations sécuritaires requises sur lesdites données.

Cette carte 1 peut donc prendre en compte le flux de données en sortie du logiciel client 2' résidant dans l'unité hôte 2 pour le soumettre aux opérations sécuritaires et le transmettre ensuite, sécurisé, aux couches logicielles assurant, en association avec l'interface 3, le transport de la même unité hôte 2.

De manière symétrique, cette carte 1 peut également prendre en compte le flux de données en sortie des couches logicielles de transport de l'unité hôte 2 (en association avec l'interface 3) pour le soumettre aux opérations sécuritaires et le transmettre ensuite, sécurisé, au logiciel client 2' résident concerné.

Pour éviter tout ralentissement excessif de la transmission des informations, il y a lieu de veiller à ce que les protocoles de transfert et les moyens de traitement matériels présents sur la carte 1 présentent une rapidité d'exécution adaptée au flux maximal susceptible d'être échangé entre unité hôte 2 et carte 1.

Si l'on se base sur un protocole rapide de type Ethernet ou GPRS sur support radio de type UMTS, les débits peuvent atteindre plusieurs Mégabits par seconde, ce qui implique que l'architecture interne de la carte doit être conçue de manière à ralentir au minimum les flux de données (des solutions cryptographiques de type DES cablé, mémoire RAM 16 ou 32 KOctets, Cache CPU et CPU 32 bits sont à envisager).

La carte 1 constituera par conséquent un tampon sécuritaire amovible de l'unité hôte 2, dont les fonctionnalités pourront être personnalisées en fonction du possesseur de la carte (possibilité de création de différents niveaux sécuritaires avec une même unité hôte 2) et dont la rupture de connexion avec l'unité hôte 2 peut, selon une variante de réalisation de l'invention (voir figure 2), entraîner une isolation totale, matérielle et logicielle, entre l'interface de communication 3 et les logiciels résidents 2'.

Au cours de certaines transactions entre un serveur ou une unité hôte distant(e) et l'unité hôte 2 connectée à la carte 1, ledit serveur peut transmettre un formulaire déterminé que l'utilisateur doit remplir et valider par signature électronique pour confirmer la transaction.

Un acte de piraterie connu consiste à modifier le formulaire au moment de l'étape de signature. Ainsi, l'utilisateur ne signe pas le formulaire qu'il visione ou qui est affiché, mais en fait un faux formulaire, substitué au premier, et représentant par exemple un paiement à un autre nom, vers une autre banque et/ou d'un autre montant. Une telle attaque est généralement réalisée par un logiciel de piratage du type "cheval de Troie".

Pour pallier à ce risque, l'invention propose selon une variante de réalisation, représentée à la figure 3 des dessins annexés, que ladite carte 1, ou en tout cas le ou les circuit(s) intégré(s) 1' qu'elle porte, comporte

également un moyen logiciel 5 de vérification de formulaires ou d'actes de paiement ou de validation de transaction, apte à conserver en mémoire le formulaire ou l'acte reçu du serveur ou de l'unité hôte distant(e).

Ce moyen logiciel 5 vérifie au moment de l'étape de signature qu'il n'y a pas eu de modification et que le client valide par sa signature effectivement ce qui lui a été soumis visuellement pour signature.

Cette opération de vérification peut être effectuée par extraction d'éléments statiques dudit acte ou formulaire, réalisation d'un calcul de contrôle sur ces éléments et vérification dudit calcul lorsque le logiciel résident 2' client renvoie ledit formulaire ou acte audit serveur distant.

Dans d'autres exécutions de transaction, il peut arriver que l'utilisateur reçoive une page de texte ou un document de ce type, récapitulant de la transaction en cours de règlement. Dans ces cas, lorsque l'utilisateur valide ladite transaction un script ou sous-programme est exécuté pour signer le document récapitulatif de la transaction.

Il peut alors arriver qu'un second document soit transmis pour signature (pendant le déroulement de l'étape de signature dans la carte), aboutissant à la signature et donc à la validation d'une fausse transaction. Une telle attaque est généralement exécutée, comme précédemment, par l'intermédiaire d'un logiciel type "cheval de Troie".

Pour éviter ce risque, l'invention propose que la carte 1 comporte aussi un moyen logiciel 6 de génération automatique de signature cryptée ou chiffrée.

L'opération de signature automatique (valable pour les données à signer en provenance du serveur authentifié avec lequel une session sécurisée / chiffrée est en cours), se déroule par exemple comme décrit ci-dessous.

Le serveur envoie au client (carte à puce et son unité hôte) un document qui doit être signé par ledit client. Un composant logiciel parcourt le document reçu pour y déceler un besoin de signature (une étiquette ("Tag") particulière peut par exemple permettre cette détection). Le composant logiciel peut alors présigner le document et le présenter à l'utilisateur pour confirmation. Le document signé peut ensuite être retourné au serveur. On peut noter qu'à aucun moment, l'unité hôte n'a été requise pour générer la signature.

Ainsi, le logiciel de signature a détecté, lorsque le document a été transféré dans la carte 1, ce document provenant d'un serveur distant

authentifié et aucun autre document ne peut être signé durant cette connexion y compris sur ordre de l'unité hôte.

Si un logiciel du type "cheval de Troie" adresse une requête pour une opération de signature, cette requête sera rejetée par la couche sécuritaire 4 de la carte 1 et un message d'avertissement sera envoyé à l'utilisateur.

Ce mécanisme peut être étendu à d'autres opérations que les transactions avec un serveur distant, par exemple à des courriers électroniques envoyés par l'unité hôte 2, lorsque le logiciel résident 2' client est fiable.

Il peut également être prévu un moyen logiciel 7 adapté pour vérifier automatiquement des documents signés, notamment les signatures des documents signés provenant du réseau (ceci s'appliquant davantage aux courriers électroniques ou documents du même ordre). Pour rendre cela possible, il y a lieu d'insérer les moyens permettant au logiciel de déterminer que le document entrant est signé, déterminer quelle clef publique doit servir à la vérification du document (ce moyen peut être un hyper lien "URL" donnant l'adresse réseau) ou récupérer cette clef publique elle-même.

Enfin, la carte 1 peut comprendre additionnellement un moyen logiciel 5' de remplissage automatique des formulaires ou documents correspondants adressés par un serveur ou une unité hôte distant(e) dans le cadre d'une transaction en cours avec ce(tte) dernier(e).

Actuellement, l'utilisateur doit introduire manuellement les informations et donnés requises (par exemple : n° de carte bancaire, date d'expiration, adresse, ...), ces dernières pouvant être aisément oubliées ou mis sur un support additionnel risquant d'être égaré, perdu ou volé.

Grâce au moyen logiciel 5' de remplissage résidant sur la carte 1, ces informations et données sont prestockées dans un registre 5" adapté, sont automatiquement lues et servent à compléter les champs reconnus du document authentifié comme venant d'un serveur ou d'une unité hôte sûr(e).

L'utilisateur aura uniquement à compléter le document par des informations non présentes dans le registre ou la banque de données 5" et ensuite à valider le document dont tous les champs auront été complétés.

La présente invention a également pour objet, comme le montre la figure 4 et de manière plus schématique la figure 3 des dessins annexés, un dispositif de communication 2 comprenant une interface 3 de connexion

et de communication avec un réseau de communication, une interface 3" de connexion et de communication avec une carte à circuit(s) intégré(s), de manière à constituer une unité hôte pour cette dernière, et une couche logicielle de sécurité, ce dispositif étant caractérisé en ce qu'il comporte des moyens de commutation 10 aptes à diriger tout ou partie d'un flux de données reçues ou à émettre sur son interface réseau 3 vers ladite interface carte 3.

De manière préférentielle, lesdits moyens de commutation 10 consistent en des moyens logiciels et sont aptes à diriger ledit flux de données automatiquement vers ladite interface carte 3" lorsque certaines conditions prédéterminées sont remplies.

Selon une caractéristique de l'invention, une desdites conditions prédéterminées peut résider dans la détection d'une version plus récente de couche logicielle de sécurité 4 disponible au niveau de la carte 1.

Ainsi, cette fonction permet à l'utilisateur de bénéficier d'une version plus récente et plus perfectionnée d'une couche logicielle de sécurité en changeant simplement la carte plutôt que le dispositif hôte.

Selon une autre caractéristique de l'invention, une, ou une autre, desdites conditions prédéterminées peut résider dans la détection d'un préfixe d'adresse indiquant qu'il s'agit d'une communication sécurisée ou à sécuriser.

Conformément à un autre mode de réalisation de l'invention, représenté à la figure 2 des dessins annexés, le dispositif de communication 2 peut être dépourvu de couche de sécurité propre.

Dans ce cas, il comprend une interface 3 de connexion et de communication avec un réseau de communication et une interface 3" de connexion et de communication avec une carte 1 à circuit(s) intégré(s) 1' selon l'invention de manière à constituer une unité hôte pour cette dernière.

Ce dispositif est alors caractérisé en ce qu'il comporte des moyens de transmission forcée 10', par exemple câblés, dirigeant la totalité du flux de données reçues ou à émettre sur son interface réseau 3 vers ladite interface carte 3".

Dans un tel dispositif, la carte 1 constitue un composant essentiel et nécessaire à son fonctionnement. En effet, l'absence de carte 1 selon l'invention isole totalement les logiciels résidents 2' du dispositif 2 de l'interface 3 et des couches de transport qui y sont associées.

Selon différentes variantes de réalisation possibles de l'invention, le dispositif de communication 2, selon l'un quelconque des deux modes de réalisation décrits ci-desssus, peut par exemple consister en un terminal mobile de radiocommunication, notamment un téléphone cellulaire, en un assistant personnel numérique ou en un module de communication faisant partie d'un appareil électronique ou informatique, notamment d'un ordinateur portable.

La présente invention concerne aussi un dispositif pour l'établissement de communications sécurisées par l'intermédiaire d'au moins un réseau de communication, caractérisé en ce qu'il est constitué par l'association d'une carte 1 telle que décrite ci-dessus avec un dispositif de communication 2 tel que décrit ci-dessus, formant unité hôte pour ladite carte 1.

Dans une telle réalisation, la carte 1 intègre une couche logicielle sécuritaire 4 apte à réaliser l'ensemble des opérations sécuritaires nécessitées par l'unité hôte 2, notamment pour les données reçues et transmises par ladite au moins une interface de communication 3, sans que la clef de session ou la clef négociée entre la carte 1 et l'unité distante en communication avec l'unité hôte 2, ne soit transmise à l'unité hôte 2.

La carte 1 mise en œuvre présente préférentiellement au moins certaines des caractéristiques supplémentaires mentionnées ci-dessus.

Comme le montrent les figures 2, 3 et 4 des dessins annexés, la carte 1 est reliée à ladite unité hôte 2 par au moins deux canaux de transmission distincts, à savoir au moins un canal réseau 8 et au moins un canal d'application 9, transitant par les interfaces complémentaires 3' et 3" coopérant lors de la connexion de la carte 1 avec le dispositif de communication 2 formant unité hôte.

On note également sur la figure 3 que l'unité hôte 2 peut, le cas échéant, disposer de deux voies parallèles de communication entre les logiciels résidents 2' et l'interface et les protocoles de communication 3, à savoir une voie sécurisée passant par la carte 1 et une voie non sécurisée reliant directement les logiciels 2' à l'interface 3, pouvant correspondre respectivement à deux protocoles de transmission différents, à savoir un protocole du type HTTP (protocole de transfert en mode hypertexte) et un protocole du type SHTTP (protocole de transfert sécuritaire en mode hypertexte).

Lorsque l'unité hôte 2 comporte déjà une interface adéquate de connexion avec une carte, une modification du logiciel telle que décrite ci-après permettra l'utilisation de la couche sécuritaire 4 de la carte 1 en lieu et place de celle existant déjà dans l'unité hôte 2 (c'est à dire que l'existence d'une couche sécuritaire (de type SSL par exemple) n'est pas obligatoire). Les modifications logicielles concernent, suivant le type de connexion, la couche transport (couche 3 du modèle ISO) de telle manière que les paquets destinés à la carte 1 lui soient transmis au travers de son interface et une des couches applicatives (la couche Session le cas échéant ou encore l'applicatif directement).

Le logiciel de l'unité hôte 2 doit être modifié de telle manière que, sur détection de l'insertion d'une telle carte 1, ladite unité puisse proposer à l'utilisateur de l'utiliser. Cette détection peut se faire sur une zone de donnée qu'il sera possible de récupérer dès la mise sous tension de la carte (réponse au reset ou fichier dédié).

Un exemple d'implémentation est la réservation d'un numéro de port. Si l'on prend l'exemple du WAP, les différents numéros de port réservés correspondent tous à un type de connexion. La couche transport n'aura alors qu'à envoyer les paquets à la carte dès lors que la carte aura été choisie pour réaliser la sécurité de la mise en connexion et de la communication consécutive et que le numéro de port indique que lesdites connexion et communication doivent implémenter une telle couche.

Le déroulement de la procédure de détection du type de carte (carte actuelle ou carte 1 avec service de couche sécurisée selon l'invention), au moment de l'insertion d'une carte dans la fente d'une interface matérielle correspondante de l'unité hôte 2 ou de la mise sous tension de ladite unité 2, et des opérations consécutives va être décrit plus précisément ci-après.

Lors de l'insertion de la carte ou de la mise sous tension de l'unité hôte 2 (avec exécution des initialisations propres à ladite unité), cette dernière est tout d'abord mise sous tension.

Deux situations peuvent alors se présenter :

- la carte envoie à l'unité une séquence d'authentification. Dans ce cas, l'unité 2 analyse cette séquence et vérifie que la carte concernée fournit bien une couche de sécurité pour des connexions à des serveurs sécurisés.

- La carte ne réagit pas à sa mise sous tension (au moins du point de vue de l'unité hôte). Dans ce cas, ladite unité 2 va chercher les informations décrivant les fonctions et les spécificités de la carte insérée au moyen d'une commande spéciale (lecture de fichier ou analogue).

Dans les deux cas précités, si la carte propose le service de couche sécurisée, l'unité hôte 2 peut positionner une variable ou mettre à 1 un indicateur analogue (drapeau), lui permettant ainsi de signifier aux couches ou logiciels concerné(e)s que les communications avec un serveur sécurisé devront s'appuyer sur les services sécuritaires de cette carte 1, c'est-à-dire diriger les données et informations provenant du ou destinées au serveur sécurisé connecté, vers ladite carte 1.

Cet aiguillage peut soit être réalisé automatiquement (comme explicité précédemment - solution préférée), soit éventuellement sur décision de l'utilisateur suite à un dialogue homme-machine.

Un déroulement possible d'une procédure de mise en communication avec un serveur sécurisé et le début de la transmission consécutive sont illustrés, à titre d'exemple, sur l'ordinogramme de la figure 5 des dessins annexés.

Enfin, la présente invention concerne additionnellement un système de communication pour l'échange de données sécurisées, ledit système comprenant au moins un dispositif formé par l'association d'une carte 1 et d'un dispositif de communication 2 tels que décrits précédemment, relié par l'intermédiaire d'un réseau de communication (radio, filaire, mixte ou autre) à un autre dispositif analogue ou à un serveur ou une unité sécurisé(e).

Bien entendu, l'invention n'est pas limitée aux modes de réalisation décrits et représentés aux dessins annexés. Des modifications restent possibles, notamment du point de vue de la constitution des divers éléments ou par substitution d'équivalents techniques, sans sortir pour autant du domaine de protection de l'invention.

REVENDICATIONS

1) Carte à circuit(s) intégré(s) comportant une interface de connexion et de communication destinée à établir une communication avec une unité hôte sous la forme d'un dispositif de communication et des moyens logiciels cryptographiques pour réaliser des calculs cryptographiques, caractérisée en ce que le(s) circuit(s) intégré(s) (1') comporte(nt) en outre une couche logicielle de sécurité ou sécuritaire (4) apte à coopérer avec lesdits moyens logiciels cryptographiques (4') pour réaliser un ensemble d'opérations sécuritaires sur les données reçues et à émettre via l'interface de connexion et de communication (3') de ladite carte (1).

2) Carte selon la revendication 1, caractérisée en ce que ladite couche logicielle de sécurité (4) comporte une fonction ou un groupe de fonctions permettant une négociation d'algorithme et de clé, ainsi qu'une fonction de chiffrement et déchiffrement.

3) Carte selon la revendication 2, caractérisée en ce que la couche logicielle de sécurité (4) comporte en outre une fonction d'authentification de certificat.

4) Carte selon l'une quelconque des revendications 1 à 3, caractérisée en ce que ladite couche logicielle de sécurité (4) est, en coopération avec lesdits moyens logiciels cryptographiques (4'), apte à réaliser un ensemble d'opérations sécuritaires permettant une sécurité de communication de type "internet".

5) Carte selon l'une quelconque des revendications 1 à 4, caractérisée en ce que ladite couche logicielle de sécurité (4) est choisie dans le groupe formé par les couches de type SSL, TLS, WTLS ou analogue.

6) Carte selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'elle comporte une mémoire pour le stockage de la clé de chiffrement/déchiffrement dont l'accès en lecture est uniquement autorisé pour ladite couche de sécurité (4).

7) Carte selon l'une quelconque des revendications 1 à 6, caractérisée en ce que ladite couche logicielle de sécurité (4) est apte à traiter la totalité, ou le cas échéant au moins une partie, des flux de données entrant et sortant par au moins une interface de communication (3) de ladite

unité hôte (2) assurant la connexion de cette dernière à un réseau de communication, en réalisant les opérations sécuritaires requises sur lesdites données.

8) Carte selon l'une quelconque des revendications 1 à 7, caractérisée en ce qu'elle comporte également un moyen logiciel (5) de vérification de formulaires ou d'actes de paiement ou de validation de transaction.

9) Carte selon l'une quelconque des revendications 1 à 8, caractérisée en ce qu'elle comporte également un moyen logiciel (6) de génération automatique de signature.

10) Carte selon l'une quelconque des revendications 1 à 9, caractérisée en ce qu'elle comprend un moyen logiciel (5') de remplissage automatique de formulaires ou de documents correspondants.

11) Carte selon l'une quelconque des revendications 1 à 10, caractérisée en ce qu'elle intègre un moyen logiciel (7) de vérification automatique de documents signés.

12) Dispositif de communication comprenant une interface de connexion et de communication avec un réseau de communication, une interface de connexion et de communication avec une carte à circuit(s) intégré(s) selon l'une quelconque des revendications 1 à 11, de manière à constituer une unité hôte pour cette dernière, et une couche logicielle de sécurité, dispositif caractérisé en ce qu'il comporte des moyens de commutation (10) aptes à diriger tout ou partie d'un flux de données reçues ou à émettre sur son interface réseau (3) vers ladite interface carte (3").

13) Dispositif selon la revendication 12, caractérisé en ce que les moyens de commutation (10) consistent en des moyens logiciels et sont aptes à diriger ledit flux de données automatiquement vers ladite interface carte (3") lorsque certaines conditions prédéterminées sont remplies.

14) Dispositif selon la revendication 13, caractérisé en ce qu'une desdites conditions prédéterminées réside dans la détection d'une version plus récente de couche logicielle de sécurité (4) disponible au niveau de la carte (1).

15) Dispositif selon la revendication 13 ou 14, caractérisé en ce qu'une desdites conditions prédéterminées réside dans la détection d'un préfixe d'adresse indiquant qu'il s'agit d'une communication sécurisée ou à sécuriser.

16) Dispositif de communication comprenant une interface de connexion et de communication avec un réseau de communication et une interface de connexion et de communication avec une carte à circuit(s) intégré(s) selon l'une quelconque des revendications 1 à 11 de manière à constituer une unité hôte pour cette dernière, dispositif caractérisé en ce qu'il comporte des moyens de transmission forcée (10') dirigeant la totalité du flux de données reçues ou à émettre sur son interface réseau (3) vers ladite interface carte (3").

17) Dispositif selon l'une quelconque des revendications 12 à 16, caractérisé en ce qu'il consiste en un terminal mobile de radiocommunication, notamment un téléphone cellulaire.

18) Dispositif selon l'une quelconque des revendications 12 à 16, caractérisé en ce qu'il consiste en un assistant personnel numérique.

19) Dispositif selon l'une quelconque des revendications 12 à 16, caractérisé en ce qu'il consiste en un module de communication faisant partie d'un appareil électronique ou informatique, notamment d'un ordinateur portable.

20) Dispositif pour l'établissement de communications sécurisées par l'intermédiaire d'au moins un réseau de communication, caractérisé en ce qu'il est constitué par l'association d'une carte selon l'une quelconque des revendications 1 à 11 avec un dispositif de communication selon l'une quelconque des revendications 12 à 19.

21) Système de communication pour l'échange de données sécurisées, ledit système comprenant au moins un dispositif selon la revendication 20, relié par l'intermédiaire d'un réseau de communication à un autre dispositif selon la revendication 20 ou à un serveur ou une unité sécurisé(e).

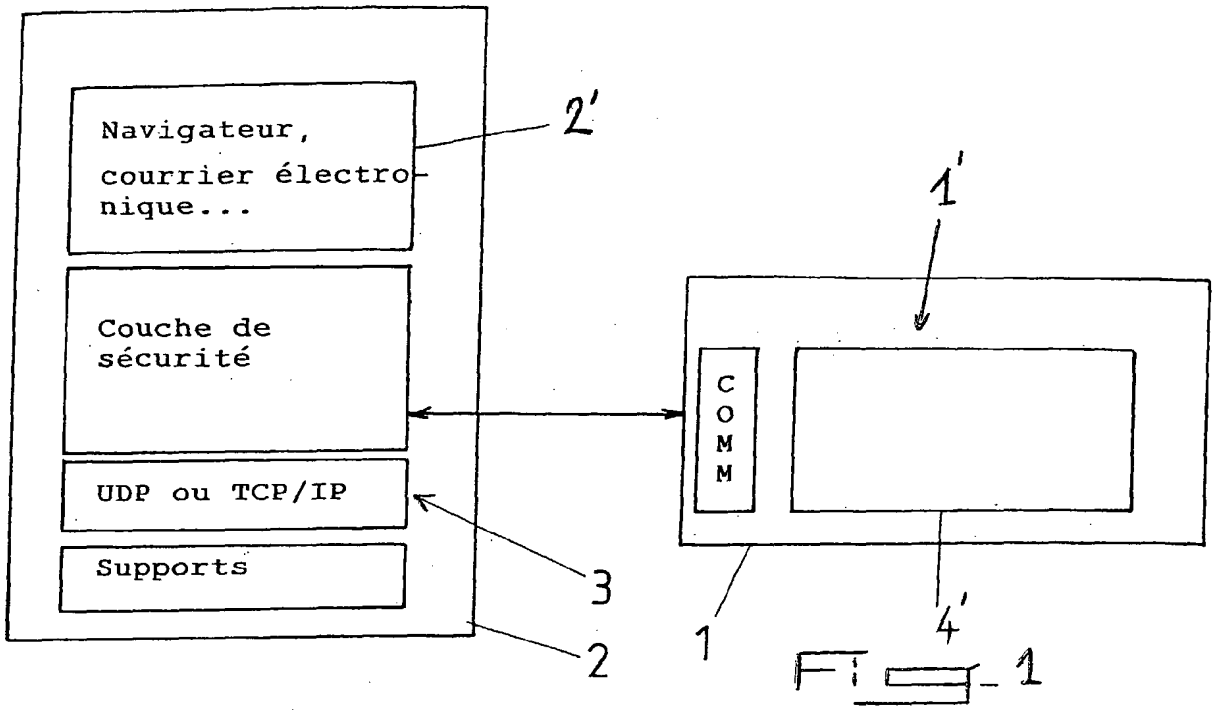

Navigateur, courrier électronique...
2'
Couche de sécurité
UDP ou TCP/IP
Supports
3
2
1'
COMM
1
4'

Fig_1

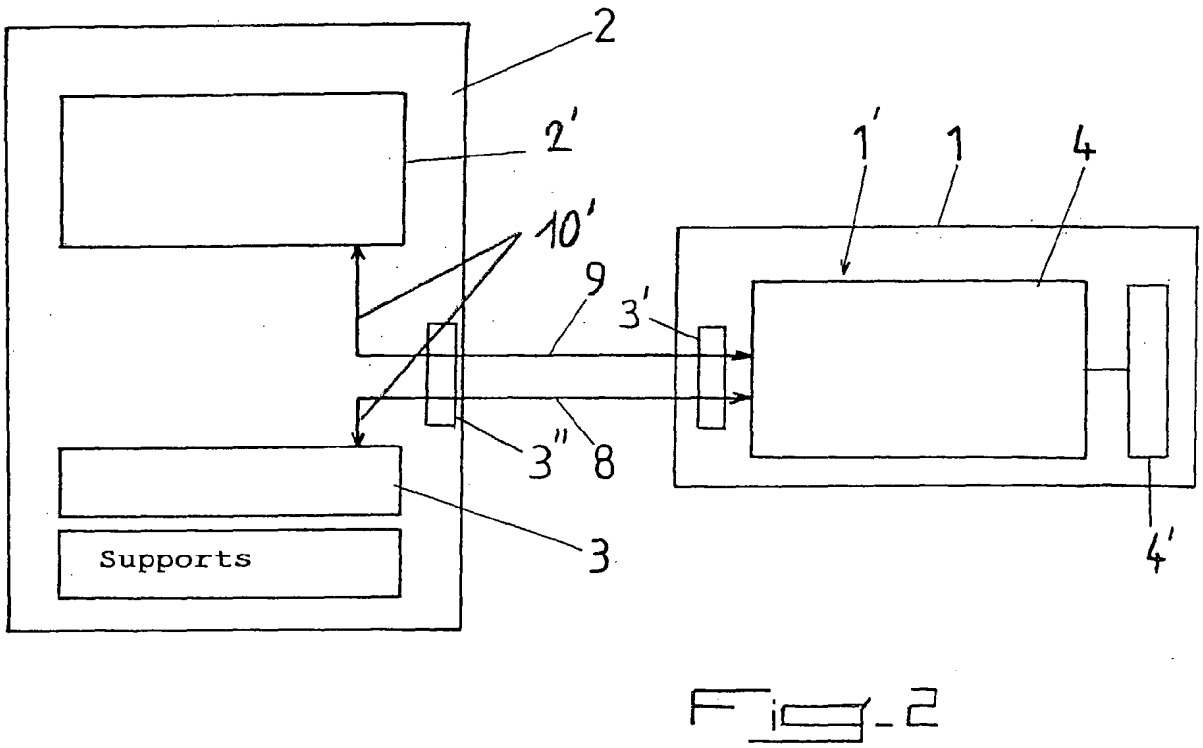

2
2'
10'
9
3'
3"
8
3
Supports
1'
1
4
4'

Fig_2

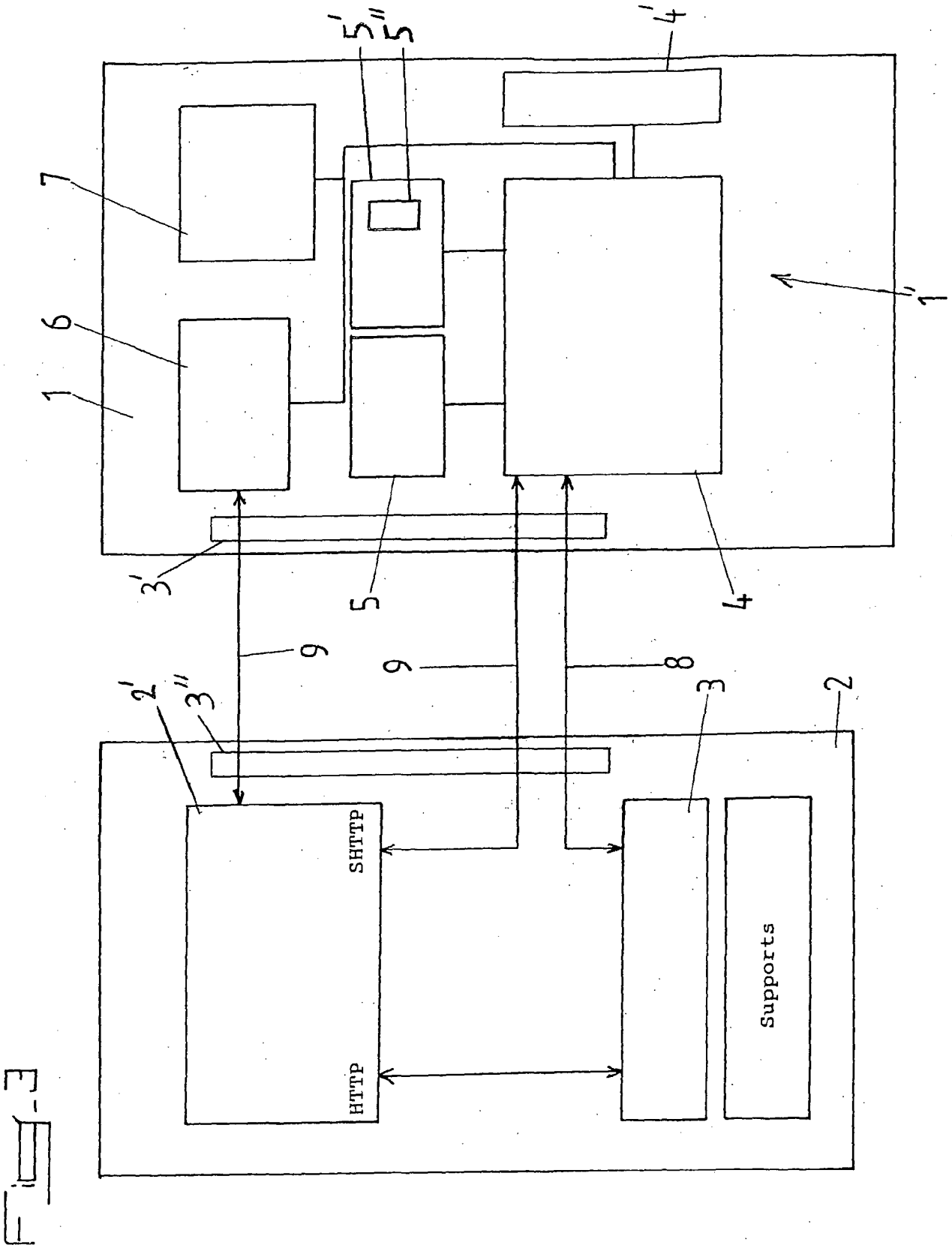


Fig-3

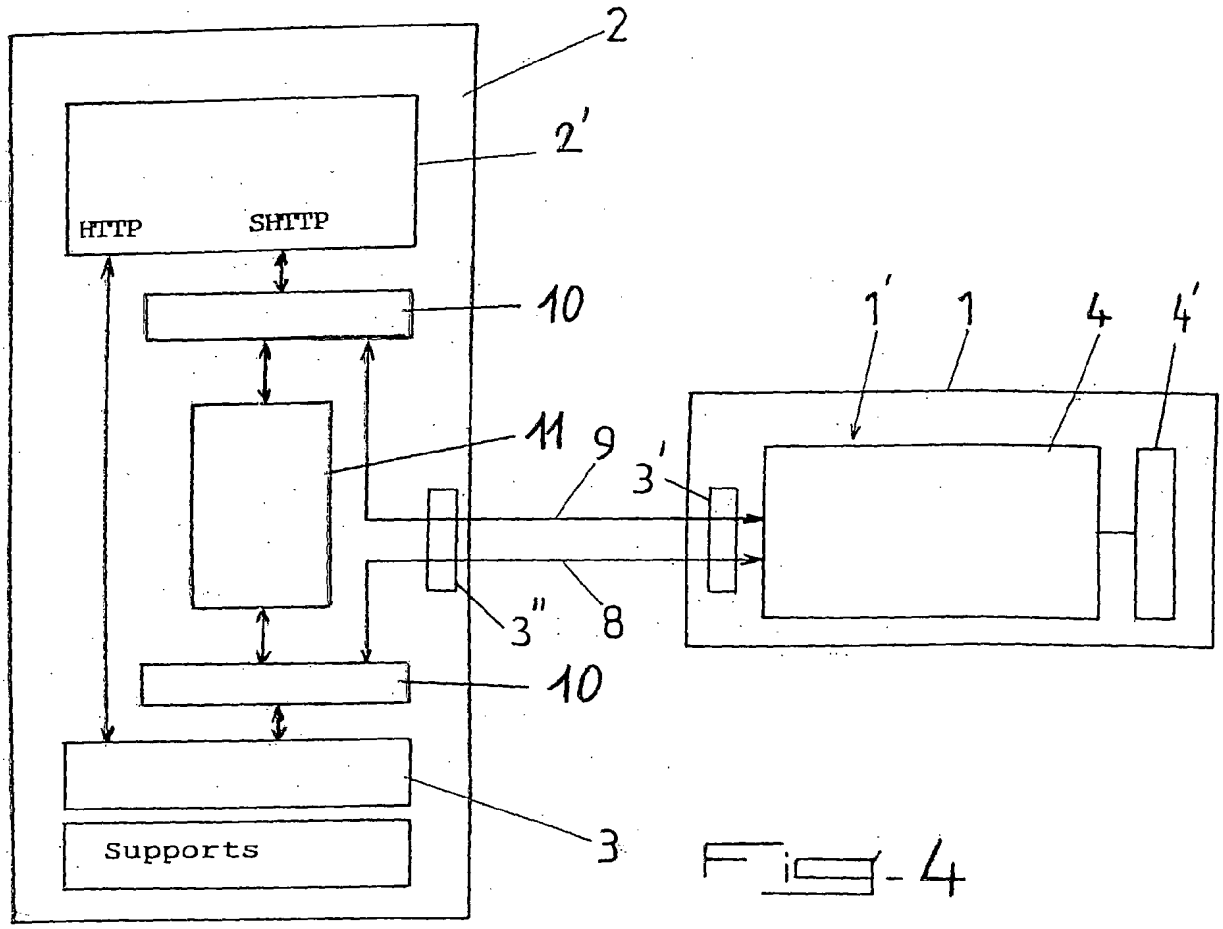


Fig-4

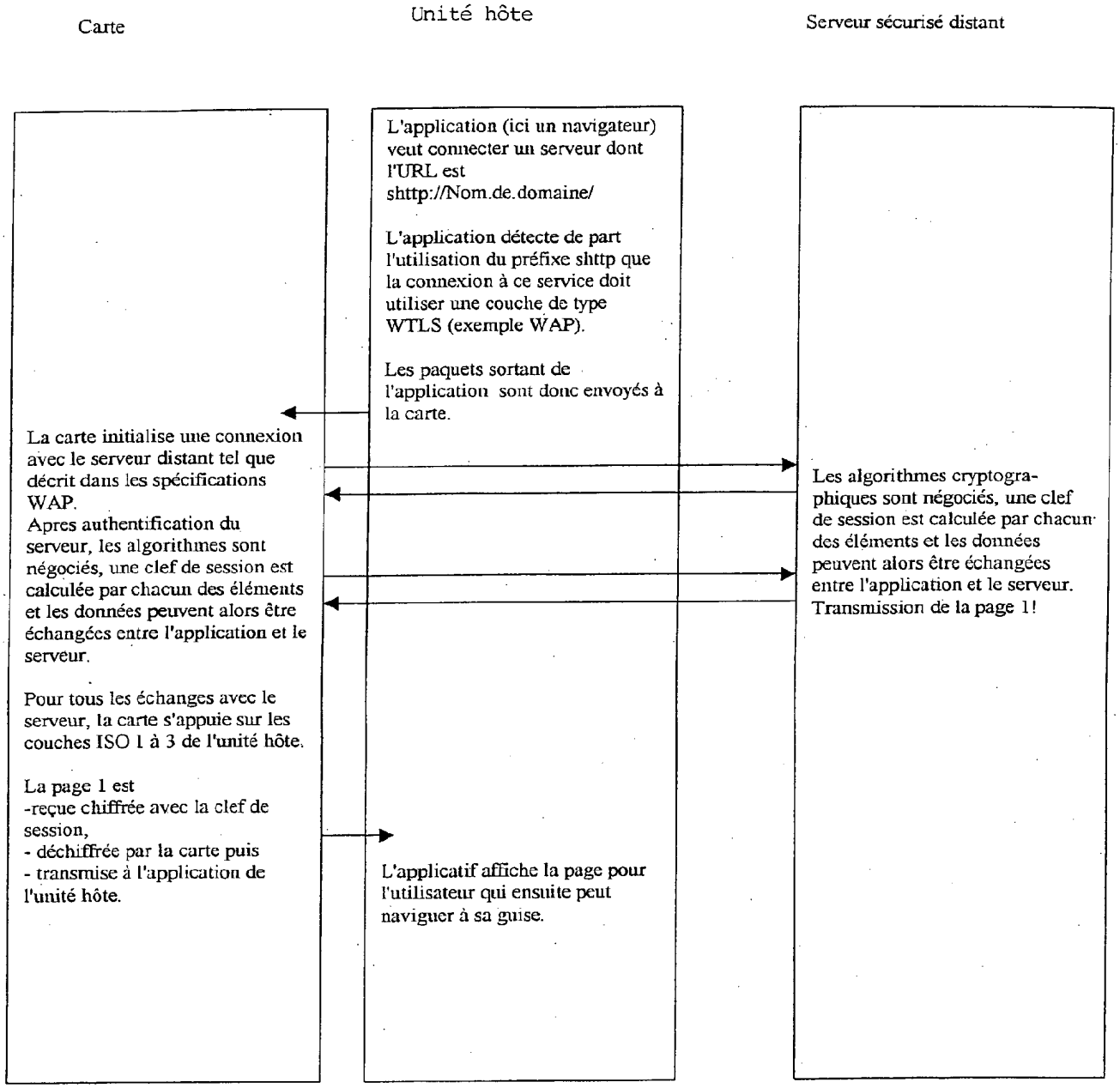

Carte
Unité hôte
Serveur sécurisé distant
L'application (ici un navigateur) veut connecter un serveur dont l'URL est shttp://Nom.de.domaine/
L'application détecte de part l'utilisation du préfixe shttp que la connexion à ce service doit utiliser une couche de type WTLS (exemple WAP).
Les paquets sortant de l'application sont donc envoyés à la carte.
La carte initialise une connexion avec le serveur distant tel que décrit dans les spécifications WAP.
Apres authentification du serveur, les algorithmes sont négociés, une clef de session est calculée par chacun des éléments et les données peuvent alors être échangées entre l'application et le serveur.
Pour tous les échanges avec le serveur, la carte s'appuie sur les couches ISO 1 à 3 de l'unité hôte.
La page 1 est
-reçue chiffrée avec la clef de session,
- déchiffrée par la carte puis
- transmise à l'application de l'unité hôte.
Les algorithmes cryptographiques sont négociés, une clef de session est calculée par chacun des éléments et les données peuvent alors être échangées entre l'application et le serveur.
Transmission de la page 1!
L'applicatif affiche la page pour l'utilisateur qui ensuite peut naviguer à sa guise.

Fig.5

INTERNATIONAL SEARCH REPORT

Interna I Application No
PCT/FR 02/00306

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 64205 A (LIUKKONEN JUKKA ;MIETTINEN JARMO (FI); NORDBERG MARKO (FI); SONERA) 26 October 2000 (2000-10-26) page 11, line 1 -page 13, line 19 figures 1,2	1-7,9, 12-21
Y	---	8,10,11
Y	WO 99 64996 A (LANDIS & GYR COMMUNICATIONS S ;CAMBOIS ETIENNE (FR)) 16 December 1999 (1999-12-16) abstract; figure 1	8,10,11

X	EP 0 889 450 A (GRP D INTERET PUBLIC CARTE DE ;SCHLUMBERGER IND SA (FR)) 7 January 1999 (1999-01-07) the whole document	1-4,6,7, 9,12,13, 16,20,21

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 May 2002	05/06/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Papastefanou, E

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 52163 A (MONDEX INT LTD) 19 November 1998 (1998-11-19) page 7, line 15 -page 8, line 21 page 10, line 15 -page 13, line 14 -----	1-7,9, 12-21

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern al Application No
PCT/FR 02/00306

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0064205 A	26-10-2000	FI 990846 A	16-10-2000
		AU 3970200 A	02-11-2000
		EP 1175799 A1	30-01-2002
		WO 0064205 A1	26-10-2000
WO 9964996 A	16-12-1999	AU 3841999 A	30-12-1999
		EP 1082710 A1	14-03-2001
		WO 9964996 A1	16-12-1999
		TW 413799 B	01-12-2000
EP 0889450 A	07-01-1999	FR 2765709 A1	08-01-1999
		CA 2242804 A1	04-01-1999
		EP 0889450 A1	07-01-1999
WO 9852163 A	19-11-1998	US 6230267 B1	08-05-2001
		AU 736325 B2	26-07-2001
		AU 6299698 A	09-09-1998
		AU 7776798 A	08-12-1998
		AU 7776898 A	08-12-1998
		AU 7776998 A	08-12-1998
		AU 7777098 A	08-12-1998
		AU 7777198 A	08-12-1998
		AU 7777298 A	08-12-1998
		AU 7777398 A	08-12-1998
		AU 7777498 A	08-12-1998
		EP 0963580 A1	15-12-1999
		EP 0981807 A2	01-03-2000
		EP 0985202 A1	15-03-2000
		EP 0985203 A1	15-03-2000
		EP 0976114 A2	02-02-2000
		EP 0985204 A1	15-03-2000
		EP 0981805 A1	01-03-2000
		WO 9837526 A1	27-08-1998
		WO 9852158 A2	19-11-1998
		WO 9852159 A2	19-11-1998
		WO 9852160 A2	19-11-1998
		WO 9852161 A2	19-11-1998
		WO 9852152 A2	19-11-1998
		WO 9852162 A2	19-11-1998
		WO 9852163 A2	19-11-1998
		WO 9852153 A2	19-11-1998
		JP 2001513231 T	28-08-2001
		JP 2001525956 T	11-12-2001
		JP 2001527674 T	25-12-2001
		JP 2001525957 T	11-12-2001
		JP 2002512715 T	23-04-2002
		JP 2001527675 T	25-12-2001
		JP 2001525958 T	11-12-2001
		US 2002050528 A1	02-05-2002
		US 6220510 B1	24-04-2001
		US 6385723 B1	07-05-2002
		US 6164549 A	26-12-2000
		US 6317832 B1	13-11-2001
		US 6328217 B1	11-12-2001
		US 2001056536 A1	27-12-2001

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 02/00306

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 00 64205 A (LIUKKONEN JUKKA ;MIETTINEN JARMO (FI); NORDBERG MARKO (FI); SONERA) 26 octobre 2000 (2000-10-26) page 11, ligne 1 -page 13, ligne 19 figures 1,2	1-7,9, 12-21
Y	---	8,10,11
Y	WO 99 64996 A (LANDIS & GYR COMMUNICATIONS S ;CAMBOIS ETIENNE (FR)) 16 décembre 1999 (1999-12-16) abrégé; figure 1	8,10,11

X	EP 0 889 450 A (GRP D INTERET PUBLIC CARTE DE ;SCHLUMBERGER IND SA (FR)) 7 janvier 1999 (1999-01-07) le document en entier	1-4,6,7, 9,12,13, 16,20,21

	-/--	

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" *document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)*

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
28 mai 2002	05/06/2002

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Papastefanou, E

1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 02/00306

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
X	WO 98 52163 A (MONDEX INT LTD) 19 novembre 1998 (1998-11-19) page 7, ligne 15 -page 8, ligne 21 page 10, ligne 15 -page 13, ligne 14 -----	1-7,9, 12-21

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demand ernationale No
PCT/FR 02/00306

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0064205 A	26-10-2000	FI 990846 A	16-10-2000
		AU 3970200 A	02-11-2000
		EP 1175799 A1	30-01-2002
		WO 0064205 A1	26-10-2000
WO 9964996 A	16-12-1999	AU 3841999 A	30-12-1999
		EP 1082710 A1	14-03-2001
		WO 9964996 A1	16-12-1999
		TW 413799 B	01-12-2000
EP 0889450 A	07-01-1999	FR 2765709 A1	08-01-1999
		CA 2242804 A1	04-01-1999
		EP 0889450 A1	07-01-1999
WO 9852163 A	19-11-1998	US 6230267 B1	08-05-2001
		AU 736325 B2	26-07-2001
		AU 6299698 A	09-09-1998
		AU 7776798 A	08-12-1998
		AU 7776898 A	08-12-1998
		AU 7776998 A	08-12-1998
		AU 7777098 A	08-12-1998
		AU 7777198 A	08-12-1998
		AU 7777298 A	08-12-1998
		AU 7777398 A	08-12-1998
		AU 7777498 A	08-12-1998
		EP 0963580 A1	15-12-1999
		EP 0981807 A2	01-03-2000
		EP 0985202 A1	15-03-2000
		EP 0985203 A1	15-03-2000
		EP 0976114 A2	02-02-2000
		EP 0985204 A1	15-03-2000
		EP 0981805 A1	01-03-2000
		WO 9837526 A1	27-08-1998
		WO 9852158 A2	19-11-1998
		WO 9852159 A2	19-11-1998
		WO 9852160 A2	19-11-1998
		WO 9852161 A2	19-11-1998
		WO 9852152 A2	19-11-1998
		WO 9852162 A2	19-11-1998
		WO 9852163 A2	19-11-1998
		WO 9852153 A2	19-11-1998
		JP 2001513231 T	28-08-2001
		JP 2001525956 T	11-12-2001
		JP 2001527674 T	25-12-2001
		JP 2001525957 T	11-12-2001
		JP 2002512715 T	23-04-2002
		JP 2001527675 T	25-12-2001
		JP 2001525958 T	11-12-2001
		US 2002050528 A1	02-05-2002
		US 6220510 B1	24-04-2001
		US 6385723 B1	07-05-2002
		US 6164549 A	26-12-2000
		US 6317832 B1	13-11-2001
		US 6328217 B1	11-12-2001
		US 2001056536 A1	27-12-2001